Before the
Federal Communications Commission
Washington, DC

In the Matter of: **Protecting the Privacy of Customers of Broadband and Other Telecommunications Services**	WC Docket No. 16-106

Reply Comments of

Paul Ohm

via electronic filing
June 22, 2016

Summary

Several comments submitted in this proceeding rely on old and outdated privacy research, to the extent they rely on research at all. These comments neglect key developments from the past decade and thus draw conclusions and make arguments that are undercut by more recent work. Because it is essential for the Commission to ground its rulemaking in sound research, I offer these reply comments to note three areas in which the ground has shifted beneath the feet of some commenters:

(1) *The true effects of encryption.* Commenters are wrong when they suggest that the surveillance of encrypted Internet communications poses no threat to privacy. Broadband Internet Access Service (BIAS) providers can still gather a staggeringly large amount of private and sensitive information about users who use encrypted communications.

Also, data that contains so little information about individuals that it cannot be used to harm privacy is data that is also not useful in other ways, for example for advertising.[1] In the far-fetched world in which a BIAS provider can no longer observe the activity of its users—say because all of its users have adopted Virtual Private Network (VPN) technology—the provider also no longer possesses any information it can monetize. A Commission rule that protects the privacy of information collected by a BIAS provider will pose almost no adverse financial burden on this kind of hypothetical BIAS provider.

(2) *The true effects of opt-in rules.* The Commission should not water down its proposal for an opt-in rule. Contrary to what commenters suggest, default choices are not immutable

---

[1] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).

destiny. In fact, recent research suggests that default choices can sometimes be slippery rather than sticky.[2] In particular, when regulators order a default choice that companies dislike, affected companies can use messaging tactics to convince large numbers of customers to switch away from the default. The relationship between BIAS providers and their customers present all of the conditions that suggest that default rules will be slippery rather than sticky.[3]

Unfortunately, the reverse has not been proved to be true: when a regulator selects an opt-out rule, the conditions leading to slippery defaults do not apply. Opt-outs are thus governed by older research, which suggests that the default choice will be sticky, meaning consumers will become trapped by it, even against their true preferences. Taken together, these studies strongly support the Commission's proposal to use an opt-in rule. The Commission should not waver from this proposal.

(3) *Bright lines are better than narrow rules protecting only sensitive information.* Finally, several commenters urge the Commission to impose opt-in rules only for sensitive information. This is a very bad idea. A rule that varies based on sensitivity will be a much more complex, unpredictable, and less privacy protective one.[4] Determining whether information is sensitive requires far more invasion of privacy as well as far more surveillance. The Commission was wise to propose rules that draw bright lines of privacy.

---

[2] Lauren E. Willis, *When Nudges Fail: Slippery Defaults*, 80 U. CHI. L. REV. 1155 (2013).
[3] *Id.* at 1200-10.
[4] Paul Ohm, *Sensitive Information*, 80 S. CAL. L. REV. 1125 (2015).

Table of Contents

Discussion

The Commission's proposed rules to protect the privacy of customers of BIAS providers are well-justified, measured, and modest. If the final rules follow the proposal, they will help give consumers what they have repeatedly asked for and deserve: a modicum of choice and control over the way information about them is collected and used online.

I am a Professor at the Georgetown University Law Center, Faculty Director of the Center on Privacy and Technology, and a noted expert in information privacy law.[5] In an earlier filing, I submitted a written statement that offered support for the underpinnings of the Commission's proposal.[6] In these reply comments, I respond to arguments that have been made by other commenters. Many commenters who have criticized the proposal rely on old or outdated research. Privacy is a dynamic field of study, and it is therefore imperative that the Commission rely on contemporary research.

A proper view of the research suggests three conclusions that the Commission should feel confident embracing, despite commenters arguments to the contrary: (1) The spread of encryption gives the Commission no reason to water down its proposed privacy rules; (2) The Commission should resist any calls to switch its proposed opt-in rule to an opt-out rule instead;

---

[5] To my surprise (and amusement), another commenter named Paul Ohm has recently filed comments in this proceeding. *See* https://www.fcc.gov/ecfs/filing/60002044828. I wanted to set the record straight that he is not me.

[6] My earlier ex parte notice in this proceeding placed my written testimony to the House Subcommittee on Communications and Technology, Committee on Energy and Commerce into the Commission's record. Ex Parte Notice by Paul Ohm in re: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106 (June 19, 2016).

and (3) The Commission should create an easy-to-apply bright line rather than vary rules based on the sensitivity of information.

I. The spread of encryption gives the Commission no reason to water down its proposed privacy rules.[7]

A number of commenters who oppose the Commission's proposed privacy rules point to the rise of encryption to argue that strong privacy protections are not necessary.[8] The Commission should disregard these arguments. A BIAS provider can monitor staggeringly large quantities of sensitive and private activity even of a customer who uses encryption.

In addition, the privacy-invasiveness of data is related directly to the value of that data for other uses such as advertising. If commenters correctly predict that BIAS providers are losing the ability to invade privacy due to encryption (a premise I seriously doubt), they are also conceding that the regulatory burden of the proposed rule will be minimal, because there will be so little benefit to lose.

A. BIAS providers can monitor sensitive and private activity even when connections are encrypted.

Encryption of online communications is, by some accounts, on the rise. At least twenty commenters discussed a report authored by a team led by Peter Swire ("Broadband for America report").[9] This lengthy report examines, among other things, the extent to which BIAS providers

---

[7] This section relates to statements or questions presented in the NPRM in paragraphs 4, 50, and 132, among others. It also relates to discussions in footnotes 80 and 238 of the NPRM.
[8] For a partial list of specific commenters who make this argument, see *infra* notes 9 and 16.
[9] Peter Swire, et al., Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others (May 2016) [*hereinafter* Broadband for America report]. According to a search performed on June 20, 2016, using the Commissions' newly upgraded ECFS search engine, https://www.fcc.gov/ecfs/, the Broadband for America report had been

can observe the activity of users. It claims that "ISPs . . . can see only narrowing subsets of the URLs and content that flow to users." and thus concludes that "ISPs today and in the future face blockades to their technical ability to view users' Internet activity."[10] The report points to both the spread of encryption and the rising number of consumers who subscribe to two or more separate broadband providers as contributing factors.[11] Although the report does not attempt to quantify precisely how much information an ISP can see, one oft-cited statistic is that "[a]n estimated 70 percent of traffic will be encrypted by the end of 2016."[12]

Even if the figures provided in the Broadband for America report are accurate, however, there is a great deal of private and sensitive information that remains exposed to BIAS providers. In my earlier filing, I noted that even with encrypted traffic, BIAS providers possess a significant power to track user behavior, particularly by observing the domain names of websites visited by users.[13] Other experts have made similar observations.[14] This renders the Broadband for

---

cited in twenty-two filings in this proceeding. As a selection from among these, the report was cited in the filed comments by trade associations (CTIA, ITIF, and Internet Commerce Coalition), corporations (Comcast, T-Mobile, AT&T, CenturyLink), and individuals (Howard Beales, Jon Leibowitz).

[10] Broadband for America report, *supra* note 9, at 35.

[11] The report points also to the fact that consumers tend to use multiple devices to access the Internet. *E.g.*, *id.* at 24-25. I am unclear why this matters beyond the fact that multiple devices might connect via different BIAS providers, which is separately accounted for in the report. Unlike edge providers, BIAS providers have no difficulty correlating communications from two different devices to a single customer or household. Multiple devices are thus a reason BIAS providers possess more power to invade privacy than edge providers, not less.

[12] *Id.*at 3.

[13] Paul Ohm, Statement of Paul Ohm Before the Subcommittee on Communications and Technology, Committee on Energy and Commerce, U.S. House of Representatives at 4 (June 14, 2016), filed in current proceeding as ex parte submission, Ohm *supra* note 6.

[14] Upturn, What ISPs Can See: Clarifying the Technical Landscape of the Broadband Privacy Debate (March 2016), https://www.teamupturn.com/reports/2016/what-isps-can-see; Nick

America report a bit of a non sequitur for this proceeding: BIAS providers retain a significant ability to invade individual privacy, even acknowledging the market and technological changes alleged in the report.

B. If encryption decreases the potential for privacy invasion, it also decreases the burden of regulation.

Those who cite the Broadband for America report in support of calls to weaken the FCC's proposal have gone one step further, making arguments that go beyond the report itself, arguments that undercut themselves. For example, the Broadband for America report notes that users who use a Virtual Private Network can, if they configure things correctly,[15] hide even the domain names of the sites they visit from their BIAS provider. Some have used this VPN effect to raise the specter that BIAS providers are on the road to becoming blinded to nearly all information about their users' habits.[16]

Feamster, *What Your ISP (Probably) Knows About You*, FREEDOM TO TINKER BLOG, March 4, 2016, https://freedom-to-tinker.com/blog/feamster/what-your-isp-probably-knows-about-you/.

[15] Broadband for America report, *supra* note 9, at 34. Professor Feamster notes that some VPN users do not configure their software correctly, thus revealing domain name information to their ISP even when using a VPN. Feamster, *supra* note 14.

[16] Comments of CenturyLink, Inc., WC Docket No. 16-106 at 8 ("While not yet pervasive, the availability of easy-to-use proxy services, including but not limited to VPNs, is clearly on the rise, and use is set to grow dramatically."); Comments of AT&T, WC Docket No. 16-106 at 28-29 ("VPN technology is growing increasingly pervasive, not only because many companies require their employees to use it, but also because more and more security-conscious consumers are signing up on their own with mass-market VPN services.").

VPNs in fact are far from becoming "pervasive." One 2014 survey cited by the Swire paper indicates that only 16% of North American users have used a VPN (or a proxy service) to connect to the Internet. Jason Mander, GWI Infographic: VPN Users, GlobalWebIndex (Oct. 24, 2014), http://www.globalwebindex.net/blog/vpn-infographic; *see* Upturn, *supra* note 14, at 10.

It is crucial for the Commission to understand that accepting this argument leads to a conclusion these commenters either do not understand or choose not to highlight: these mythical BIAS providers that lose the ability to learn about their users' habits will also not be burdened by strong privacy rules.

This is because the utility of information for advertising is directly related to the utility of information for privacy invasion.[17] Information tends to be valuable across the board or not at all. It would be surprising to encounter data that is good for advertising but not for privacy invasion or government surveillance. And as the utility decreases for one activity, it tends to decrease for the other activities too.[18]

This conclusion rests on a very old insight from information theory, work that can be adequately conveyed by some common-sense observations. The goal of advertising is to place a particular target consumer in a category of consumer preferences. The advertiser hopes to devise a system that will help differentiate this person from the crowd. This activity mirrors precisely at least one definition of privacy invasion.

This is why some acts of advertising are almost indistinguishable from invasions. The FTC, for example, noted that data brokers group individuals into categories, some based on potentially sensitive attributes, "such as 'Urban Scramble' and 'Mobile Mixers,' both of which include a high concentration of Latinos and African Americans with low incomes" and also "'Rural Everlasting, 'which includes single men and women over the age of 66 with 'low educational

---

[17] *See* Ohm, *supra* note 1, at 1752 ("Utility and privacy are, at bottom, two goals at war with one another.").

[18] This is not a universal rule. Well-designed systems can be created that, for example, reveal information for one purpose yet still protect privacy. Dwork, *Differential privacy*, 2006 PROC. INT'L COLLOQ. ON AUTOMATA, LANGUAGES AND PROGRAMMING (2006).

attainment and low net worths.'"[19] Whether this type of categorization counts as advertising or invasion is very much in the eye of the beholder.

This research means that in the extreme form with which some have characterized the Broadband for America report—a world where most users use VPNs, for example—commenters have essentially conceded that BIAS providers have very little to gain from access to the residual information they can gather. In turn, if the Commission's proposed rule applies to these providers, the providers would have almost nothing to lose.

The Commission should feel empowered by the fundamental relationship between the privacy and utility of data. If commenters are correct and BIAS providers are about to become blind to user data due to encryption, then the Commission's rule will do no harm. If, on the other hand, I (and other commenters) are correct that BIAS providers retain a significantly ability to cause privacy injury, then the rules the Commission has proposed will increase privacy for consumers in a way that more than justifies the modest regulatory burden they impose.

II. The Commission should resist any calls to switch its proposed opt-in rule to an opt-out rule instead.[20]

Some of the comments submitted suggest that the Commission's proposal to apply an opt-in rule to all information that is used for purposes other than "to market . . . communications-related services" or "in the provision of BIAS" will result in fewer subscribers being subject to

---

[19] FTC, Data Brokers: A Call for Transparency and Accountability (May 2014), https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014.

[20] This section relates to statements or questions presented in the NPRM in paragraphs 68-70, 127-33, among others.

these uses, which will result in diminished returns, higher prices for consumers, and less investment in broadband build-out, as compared to an opt-out. These arguments rely on the idea that default choices are sticky, meaning that consumers tend to remain with a default, even against their true preferences or best interests.[21] They base these arguments on research into nudges and choice architecture. But newer research suggests that default choices are sticky only in one direction. To a motivated company, the default choice of an opt-in rule tends to be slippery, while opt-out rules tend to be sticky. The Commission therefore should resist any calls to downgrade portions of its proposal from an opt-in to an opt-out standard for consent.

The best synthesis of the contemporary research is an important recent article by Professor Lauren Willis of the Loyola Law School, Los Angeles.[22] This article reveals that regulated companies can often compel or encourage consumers to opt in to behavior that is favorable to the companies, including behavior that some consider against those consumers' interests.[23] In other words, the study suggests that given the right conditions, default choices are not sticky, they are in fact quite "slippery," but only when switching benefits the company.

---

[21] *E.g.,* Comments of the National Cable & Telecommunications Association, WC Docket 16-106 at 79-80 ("Research shows that individuals are significantly more likely to choose to participate in a given activity when offered an opt-out choice rather than being asked to opt-in."); Comments of Comcast Corp., WC Docket No. 16-106 at 47-50 ("It is well understood that an opt-in consent mechanism results in far fewer individuals conveying their consent than is the case under an opt-out consent mechanism.").

[22] Willis, *supra* note 2. For my earlier thoughts on this article, see Paul Ohm, *The Care and Feeding of Sticky Defaults in Information Privacy Law*, JOTWELL, May 20, 2013, http://cyber.jotwell.com/the-care-and-feeding-of-sticky-defaults-in-information-privacy-law/.

[23] Willis, *supra* note 2. Professor Willis reverses the terminology usually embraced in privacy law debates. She refers to a rule that requires consumers to affirmatively choose to accept the behavior a rule seeks to limit as an "opt-out" rule. In privacy, we call this an "opt-in rule", and I am using the privacy conventions rather than Professor Willis's usage in this comment.

The paper focuses on a specific case study, the effects of regulatory action to protect consumers from banking fees from checking account overdraft coverage.[24] In 2010, federal regulators enacted a new rule prohibiting banks from charging overdraft fees for ATM or debit card transactions unless an account holder opted in to the overdraft protection option.[25] Regulators saw these fees as "a low-risk, high-cost loan," which could lead to a "$35 cup of coffee" and could be viewed as a loan with "an annual percentage rate (APR) of over 7,000 percent."[26]

The result of the regulation was, perhaps, somewhat surprising: a mere four months after the rule became mandatory, large numbers of consumers had opted-in to the overdraft protection. Perhaps even more surprising, heavy overdraft users, who were the ones who suffered most from the high fees, opted in at the highest rates. For some banks, as many as 66% of heavy overdraft users opted in.[27]

These results call into question an older series of famous studies that suggest the stickiness of default choices. Perhaps most famously, a series of decade-old studies suggest that employees save considerably more for retirement when the default choice enrolls them in their employer's program rather than waits for them to sign up on their own.[28] The retirement savings example serves as a centerpiece of libertarian paternalism, most notably in the work of Richard Thaler and Cass Sunstein.[29] At least when it comes to nudges and choice architecture, the commenters

---

[24] *Id.*
[25] *Id.* at 1175 *citing* 12 CFR § 205.17.
[26] *Id.* at 1176.
[27] *Id.*, at 1184.
[28] *Id.* at 1161-74 (summarizing research into default choices).
[29] RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVE DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2008).

in this proceeding seem to have internalized the lessons of a decade ago but have not yet paid attention to updated research.

Professor Willis describes in detail the varied ways in which banks have worked to convince customers to opt-in to overdraft fees. From this, she derives four factors that together suggest that default choices will be slippery rather than sticky, four factors all present in this proceeding:

> (1) one party opposes the default strongly enough to incur costs trying to make the default slippery,
>
> (2) that opposed party has access to the party the default aims to aid (typically a consumer) when the consumer is in a position to opt [in],
>
> (3) the consumer lacks clear preexisting preferences about the decision, and
>
> (4) the consumer lacks clear preexisting preferences about the decision.[30]

Because all four factors are present in the relationship and incentives of BIAS providers and consumers, it is likely that BIAS providers will be able to persuade many of their customers to opt in to uses of personal data that would not be permitted by default under the Commission's proposal. The fact that BIAS providers have an incentive to compel consumers to opt-in (factor one) has been demonstrated by the time, energy, and resources they have already invested into lobbying against this rule. A BIAS provider not only can send email and paper mail messages to its consumers, it literally controls the channel of communication between the consumer and the rest of the Internet (factor two). A BIAS provider could, for example, require the consumer to make choices upon his or her first use of the connection or on a recurring basis thereafter.

---

[30] Willis, *supra* note 2, at 1200 (spacing added).

Finally, there is an enormous body of research (summarized well in the NPRM itself) attesting to the complex consumer preferences about online privacy (factors three and four).

Unfortunately, Professor Willis's analysis suggests the slipperiness of the default choice only in one direction: when the regulator chooses an opt-in rule, a motivated company can convince consumers to opt in, in large numbers. On the other hand, this research does not suggest that an opt-out rule is likewise slippery. When consumers are subject to monitoring by default, the critical first factor—company motivation—is absent. This means that for an opt-out rule, the behavior of consumers will be characterized by the older research establishing the stickiness of default choices, meaning it is likely that consumers who would prefer to opt-out may fail to express their true preference because of consumer confusion and decision biases.

The Commission should resist any calls to switch its category of uses subject to a proposed opt-in rule to an opt-out rule instead. Companies can surmount an opt-in default choice but consumers cannot in the same way surmount an opt-out default choice. Commenters who suggest that an opt-in rule will lead to considerably greater costs to BIAS providers than an opt-out rule are neglecting this research.

III. The Commission should create an easy-to-apply bright line rather than vary rules based on the sensitivity of information.[31]

Multiple commenters have urged the Commission to water down its opt-in rule by subjecting BIAS providers to opt-in treatment for only "sensitive" information.[32] There are many reasons the Commission should disregard this suggestion.

---

[31] This subsection relates to statements or questions presented in the NPRM in paragraphs 134-38, among others.

The great virtue of the proposed opt-in rule is that it draws bright lines. This follows a pattern consistently seen in privacy laws similar to Section 222, as I noted in my earlier filing.[33] Bright lines are simpler and more inexpensive to implement than the alternatives; they lend themselves to consumer comprehensibility and confidence.

In contrast, if the Commission were to enact a rule based on the sensitivity of information, the result would likely be varying standards, great uncertainty, and consumer confusion. I have documented the way companies involved in the precise context under discussion—advertising based on online activity—have disagreed dramatically about how to define sensitive information.[34] Four groups that have attempted to define sensitive information for online advertising—Facebook, Google, the Networking Advertising Initiative ("NAI") and the Digital Advertising Alliance ("DAA")—have concocted four very different definitions. Advertisers can definitely target ads to people suffering from a particular disability on DAA platforms, definitely not on Facebook, and probably not on Google or NAI. Genomic information is only expressly prohibited within the NAI definition, arguably within Google's, and likely not Facebook's or DAA's. Ads targeted to symptoms might be barred by Google and maybe NAI, but probably not

---

[32] *E.g.,* Comments of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, WC Docket No. 16-106 at 22 ("FTC staff recommends that the FCC consider the FTC's longstanding approach, which calls for the level of choice to be tied to the sensitivity of data and the highly personalized nature of consumers' communications in determining the best way to protect consumers."); Comments of T-Mobile, WC Docket No. 16-106 at 29 ("Opt-in should be reserved very sensitive information whose use or disclosure would surprise consumers."); Comments of Verizon, WC Docket No. 16-106 at 14 ("[C]onsent to use less sensitive customer information (such as an email address, the type of service plan to which the customer subscribers, or the accessories they may have purchased) should be inferred for such first-party marketing.").

[33] Statement of Paul Ohm, *supra* note 6, at 6-7 (comparing section 222 to other "sectoral" privacy laws like HIPAA, for health care information, and FERPA, for student records).

[34] Ohm, *supra* note 4.

by Facebook or DAA.[35] There is no rhyme or reason here. This experience suggests that if customers were protected by an opt-in rule for sensitive information alone, Comcast, AT&T, Time Warner, Verizon, etc., would each come up with its own definition, one likely to differ in confusing and irrational ways from the definitions of the others.[36]

In addition, whether information is sensitive or not might vary considerably based on context. To decide whether something is sensitive or not, a responsible BIAS provider would have to increase its surveillance, collecting much more information than it would under a bright line, to fairly adjudge whether a given piece of information meets its idiosyncratic definition.[37]

Finally, commenters try to bolster their suggestion for an opt-in rule for sensitive information as a way the Commission could harmonize its actions with the FTC's approach.[38] This does not follow, because the FTC can police opt-in versus opt-out practices only when they lead to deception or unfairness. The FTC has never said that it is inherently unfair under Section 5 to adopt an opt-out rule for sensitive information, as far as I know. The FTC's "rule" is simply a "best practice," recited in the 2012 Privacy Report and other policy documents.[39] Requiring opt-

---

[35] *Id.* (quoting relevant parts of the four definitions).
[36] *Id.* at 1139.
[37] *See* Comments of FTC Staff, *supra* note 32, at 22 ("[I]f the FCC were to adopt FTC staff's recommendation for opt-in consent before use of the content of consumer communications, BIAS providers would not be permitted to inspect the contents of such communications to determine whether they are sensitive.").
[38] *E.g.*, Comments of Jon Leibowitz, WC Docket No. 16-106, at 8-9; Comments of CTIA, WC Docket No. 16-106, at 8-9.
[39] FTC Report, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy Makers at iii (March 2012) ("The final framework is intended to articulate best practices for companies that collect and use consumer data."), *available at* https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses- policymakers.

in for all sensitive information would not harmonize the FCC and FTC rules, despite what commenters claim.

Respectfully submitted,

/s/

Paul Ohm